HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10004553-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Frank, et al.

Confirmation No.: 9973

Application No.: 09/759,428

Examiner: LaForgia, Christian A.

Filing Date: January 12, 2001

Group Art Unit: 2131

Title: SYSTEM AND METHOD FOR PROVIDING SECURITY PROFILE INFORMATION TO A USER OF A COMPUTER SYSTEM

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on June 9, 2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $450	☐ 3rd Month $1020	☐ 4th Month $1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: 7/6/2006

OR

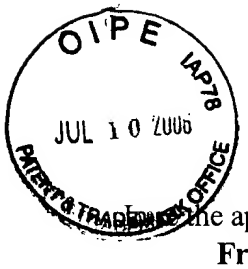
☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.
Date of facsimile:
Typed Name: Shana L. East
Signature: Shana L. East

Respectfully submitted,
Frank, et al.
By

Jon E. Holland
Attorney/Agent for Applicant(s)
Reg No.: 41,077
Date: 7/6/2006
Telephone: (256) 704-3900

AF

SFW



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the application of: **Frank, *et al.***	)	Confirmation No.: 9973
Serial No.: 09/759,428	)	Art Unit: 2131
Filed: January 12, 2001	)	Examiner: LaForgia, Christian A.
For: SYSTEM AND METHOD FOR PROVIDING SECURITY PROFILE INFORMATION TO A USER OF A COMPUTER SYSTEM	)	Docket No.: 10004553-1

APPEAL BRIEF UNDER 37 C.F.R. §1.192

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. §1.192 is submitted in support of the Notice of Appeal filed June 9, 2006, responding to the final Office Action of April 4, 2006.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those which may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Company Deposit Account No. 08-2025.

07/12/2006 SHASSEN1 00000050 082025 09759428
01 FC:1402 500.00 DA

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope, with sufficient postage, addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 20231 on

7-6-06

Signature: Shona R. Scott

I. REAL PARTY IN INTEREST

The real party in interest of the instant application is the assignee, Hewlett-Packard Development Company, L.P.

II. RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences that will affect or be affected by a decision in this appeal.

III. STATUS OF THE CLAIMS

Claims 1-28 are pending in the present application. The final Office Action of April 4, 2006, rejected claims 1-15 and 23-28 under 35 U.S.C. §103 as allegedly unpatentable over *Hayes* (U.S. Patent No. 6,339,826) in view of *Shrader* (U.S. Patent No. 6,009,475). The final Office Action also rejected claims 16-22 under 35 U.S.C. §103 as allegedly unpatentable over *Hayes* in view of *Shrader* and further in view of *Deo* (U.S. Patent No. 5,720,033).

IV. STATUS OF AMENDMENTS

No amendments have been made or requested since the mailing of the final Office Action. A copy of the current claims is attached hereto as Appendix A.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A computer system (*e.g.*, reference numeral 50) of some embodiments, such as that embodied by claim 1, comprises memory (*e.g.*, reference numeral 18) and a security application (*e.g.*, reference numeral 52). The security application is configured to display a list of security

rules for locking down resources of the computer system (*e.g.*, page 13, lines 11-19). The security application is configured to enable a set of the security rules, based on inputs from a user, and to cause the computer system to enforce the enabled set of security rules by modifying a machine state of the computer system (*e.g.*, page 13, line 19, through page 14, line 8). The security application is further configured to enable the user to select one of the security rules and to display information describing the selected rule in response to a selection of the one rule from the displayed list by the user (*e.g.*, page 17, lines 11-18; page 19, lines 17-18; and Figure 3). The information is based on data stored in the memory (*e.g.*, page 19, lines 18-22, and Figure 2).

In at least one embodiment, such as that embodied by claim 3, the security application is configured to display the list within a window, and the window includes a plurality of selectable icons (*e.g.*, page 20, line 3, and Figure 3). The security application is further configured to display different sets of information describing the selected rule in response to selections of different ones of the icons (*e.g.*, page 20, lines 3-24).

In at least one embodiment, such as that embodied by claim 21, the security application is configured to simultaneously display the list in a first sub-window of the window and one of the sets of information in a second sub-window of the window (*e.g.*, page 20, lines 3-24).

In at least one embodiment, such as that embodied by claim 4, the security application is configured to display a main window. The security application is further configured to display rules of the list in a first sub-window of the main window and to display the information describing the selected rule in a second sub-window of the main window (*e.g.*, page 17, lines 1-18, and Figure 3).

In at least one embodiment, such as that embodied by claim 7, the main window includes a plurality of selectable icons, and the security application is further configured to

display in the second sub-window different sets of information describing the selected rule in response to selections of different ones of the icons (*e.g.*, page 20, lines 3-24).

In at least one embodiment, such as that embodied by claim 22, the security application is configured to simultaneously display the first and second sub-windows (*e.g.*, page 17, lines 1-18 and Figure 3).

In at least one embodiment, such as those embodied by claims 24 and 28, the information comprises help information for informing the user of an operational ramification to the system of enabling the one rule (*e.g.*, page 20, lines 5-16).

In at least one embodiment, such as that embodied by claim 25, the security application is configured to display a plurality of selectable icons simultaneously with the information. The security application is further configured to display new information describing the one rule based on the selection of the one rule and in response to a selection of one of the icons by the user (*e.g.*, page 20, lines 3-24).

In at least one embodiment, such as that embodied by claim 26, the security application is configured to display the selectable icons in the second sub-window (*e.g.*, page 20, lines 8-9, and Figure 3).

In at least one embodiment, such as that embodied by claim 27, the security application is configured to categorize the list of rules and to display categories of the rules in a third sub-window of the main window (*e.g.*, page 17, lines 1-2; page 18, lines 3-10; and Figure 3).

A computer system (*e.g.*, reference numeral 50) of some embodiments, such as that embodied by claim 8, comprises means for displaying a list of security rules for locking down resources of the computer system (*e.g.*, page 13, lines 11-19) and means for receiving inputs from a user of the computer system (*e.g.*, page 13, lines 5-6 and 19-22). The computer system also comprises means for enabling a set of the security rules based on the inputs from the user

(*e.g.*, page 13, line 19, through page 14, line 8) and means for enforcing the enabled set of security rules (*e.g.*, page 14, lines 1-8). The computer system further comprises means for selecting one of the security rules from the displayed list (*e.g.*, page 17, lines 11-13, and page 19, lines 17-18) and means for displaying information describing the selected rule in response to a selection of the one rule by the selecting means (*e.g.*, page 17, lines 13-18, and page 19, line 18, through page 20, line 2).

A method of some embodiments, such as that embodied by claim 9, for locking down resources of computer systems (*e.g.* reference numeral 50) comprises displaying a list of security rules for locking down resources of a computer system (*e.g.*, page 13, lines 11-19) and receiving inputs from a user of the computer system (*e.g.*, page 13, lines 5-6 and 19-22). The method also comprises enabling a set of the security rules based on the inputs from the user (*e.g.*, page 13, line 19, through page 14, line 8) and enforcing the enabled set of security rules (*e.g.*, page 14, lines 1-8). The method further comprises selecting one of the security rules from the displayed list (*e.g.*, page 17, lines 11-13, and page 19, lines 17-18) and displaying information describing the selected rule in response to the selecting (*e.g.*, page 17, lines 13-18, and page 19, line 18, through page 20, line 2).

In at least one embodiment, such as that embodied by claim 12, the displaying a list of security rules further comprises displaying rules of the list in a first sub-window of the main window, wherein the displaying information further comprises displaying the information describing the selected rule in a second sub-window of the main window (*e.g.*, page 17, lines 1-18, and Figure 3).

In at least one embodiment, such as that embodied by claim 18, the displaying rules of the list in a first sub-window and the displaying the information describing the selected rule in a second sub-window are performed simultaneously (*e.g.*, page 17, lines 1-18, and Figure 3).

A computer-readable medium of some embodiments, such as that embodied by claim 23, has a program, the program comprises logic for displaying a list of security rules (*e.g.*, page 13, lines 11-19) and logic for enabling a set of the security rules, based on inputs from a user (*e.g.*, page 13, line 19, through page 14, line 8). The program also comprises logic for causing a computer system to enforce the enabled set of security rules (*e.g.*, page 14, lines 1-8) and logic for enabling a user to make a selection of one of the security rules while the list of security rules, including the one security rule, is being displayed (*e.g.*, page 17, lines 11-13, and page 19, lines 17-18). The program further comprises logic for displaying information describing the selected rule in response to the selection (*e.g.*, page 17, lines 13-18, and page 19, line 18, through page 20, line 2).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-15 and 23-28 are rejected under 35 U.S.C. §103 as allegedly unpatentable over *Hayes* (U.S. Patent No. 6,339,826) in view of *Shrader* (U.S. Patent No. 6,009,475).

Claims 16-22 are rejected under 35 U.S.C. §103 as allegedly unpatentable over *Hayes* in view of *Shrader* and further in view of *Deo* (U.S. Patent No. 5,720,033).

VII. ARGUMENT

In order for a claim to be properly rejected under 35 U.S.C. §103, the combined teachings of the prior art references must suggest all features of the claimed invention to one of ordinary skill in the art. See, *e.g.*, *In Re Dow Chemical Co.*, 837 F.2d 469, 5 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1988), and *In re Keller*, 642 F.2d 413, 208 U.S.P.Q. 871, 881 (C.C.P.A. 1981). In addition, "(t)he PTO has the burden under section 103 to establish a *prima facie* case of obviousness. It can satisfy this burden only by showing some objective teaching in the prior art

or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references." *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988) (Citations omitted). Furthermore, the Federal Circuit has stated that "(i)t is impermissible, however, to simply engage in hindsight reconstruction of the claimed invention, using the applicant's structure as a template and selecting elements from references to fill the gaps." *In re Gorman*, 933 F.2d 982, 987, 18 U.S.P.Q.2d 1885 (1991).

Discussion of 35 U.S.C. §103 Rejections of Claims 1, 2, 5, 6, 8, 19, 20, and 28

Claim 1 presently stands rejected in the final Office Action under 35 U.S.C. §103 as allegedly unpatentable over *Hayes* (U.S. Patent No. 6,339,826) in view of *Shrader* (U.S. Patent No. 6,009,475). Claim 8 comprises similar claimed limitations which are missing from the alleged combination (with respect to the outstanding 35 U.S.C. §103 rejections) as claim 1. Claims 2, 5, 6, 19, 20, and 28 depend from claim 1. Therefore, claim 1 is discussed below as an exemplary claim for discussion.

Claim 1 presently reads as follows:

> 1. A computer system, comprising:
> memory; and
> a security application configured to display a list of security rules for locking down resources of said computer system, said security application configured to enable a set of said security rules, based on inputs from a user, and to cause said computer system to enforce said enabled set of security rules by modifying a machine state of said computer system, ***said security application further configured*** to enable said user to select one of said security rules and ***to display information describing said selected rule in response to a selection of said one rule from said displayed list by said user***, said information based on data stored in said memory. (Emphasis added).

Applicants respectfully assert that the combination of *Hayes* and *Shrader* fails to suggest at least the features of claim 1 highlighted above. Accordingly, the 35 U.S.C. §103 rejection of claim 1 is improper.

In rejecting claim 1, it is candidly admitted in the Office Action that *Hayes* fails to disclose "said security application further configured to enable said user to select one of said security rules and to display information describing said selected rule in response to a selection of said one rule by said user." However, it is then alleged in the Office Action that *Shrader* teaches such features of claim 1 at column 5, line 38, to column 6, line 34, and column 8, lines 5-18.

The cited sections of *Shrader* appear to disclose various "panes" that are used to display various information, and the Office Action apparently asserts that at least some of this displayed information constitutes a "list of security rules." Further, *Shrader* teaches a "ticker tape pane 260" that "provides the administrator with dynamic, statistical information about the entries and objects on the page. The information scrolls from right to left and is updated as the administrator initiates actions on the page." Column 6, lines 1-5. It is apparently the position of the Patent Office that the updating of the "ticker tape pane 260" as "the administrator initiates actions on the page" could constitute the feature of displaying information describing a "security rule in response to a selection of said one rule from said displayed list," as described by claim 1. Applicants respectfully disagree and assert that there is nothing in *Shrader* to suggest that any of the described "actions" of *Shrader* includes selection of an alleged "security rule" by a user.

In this regard, when the teachings of *Shrader* are properly considered as a whole, it appears that the described "actions" refer to those performed in response to initiation of the displayed pushbuttons, such as those shown in the "display ***action*** pane 220" and "list ***action*** pane 250." (Emphasis added). Indeed, in describing the display action pane 220, it is asserted in *Shrader* that this pane "presents ***actions*** the administrator can initiate by pushbuttons 222." (Emphasis added). Further, the very example given in *Shrader* for updating the "ticker tape pane" is that "on the IP filter page, the ticker tape pane 360 would display the number of filter

rules that matched the query and statistics about them." Column 6, lines 5-8. Notably, such a "query" is initiated by a pushbutton, similar to those shown in the display action pane 220 and the list action pane 250. See column 7, lines 58-61.

Thus, the "actions" for which the "ticker tape pane" should be updated apparently refer to those described in *Shrader* as being initiated via pushbuttons, such as those shown in panes 220 and 250. Moreover, although it appears that the "ticker tape pane" could be updated in response to a user initiation of a pushbutton, none of the pushbuttons could arguably be construed as constituting a "security rule," as recited by claim 1. Accordingly, the described updating of the "ticker tape pane" fails to suggest displaying information for describing a selected "security rule" in response to selection of such "security rule," as recited by pending claim 1.

For at least the above reasons, Applicants respectfully assert that the Office Action fails to establish that the combination of *Hayes* and *Shrader* suggests a "security application configured to... display information describing said selected rule ***in response to a selection of said one rule from said displayed list by said user***," as described by claim 1. (Emphasis added). Accordingly, the Office Action fails to establish a *prima facie* case of obviousness with respect to claim 1, and the 35 U.S.C. §103 rejection of this claim should be withdrawn.

In maintaining the rejection of claim 1, it is asserted in the final Office action that:

> "In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986)." Page 2, paragraph 3.

Applicants respectfully traverse the Office Action assertion that Applicants have argued against the references individually. In this regard, by focusing on the features of displaying "information describing said selected rule in response to a selection of said one rule from said

displayed list by said user," as set forth above, Applicants' arguments focus on features that are clearly not suggested by *Hayes*. In fact, the Examiner expressly admits that such features are not suggested by *Hayes*. In particular, it is asserted in the Office Action that "Hayes does not disclose said security application further configured to enable said user to select one of said security rules and to display information describing said selected rule in response to a selection of said one rule by said user." Page 3, paragraph 10. Moreover, in the outstanding Office Action, it is alleged that the features missing from *Hayes* are suggested by the alleged combination ***because such features are found in Shrader***. Accordingly, by establishing that *Shrader* does not, in fact, suggest the features missing from *Hayes*, Applicants have adequately traversed the rejection and have shown that the alleged combination does not suggest each feature of claim 1.

In maintaining the rejection of claim 1 it is also asserted in the Office Action that:

> "In response to applicant's argument that the references of record do not disclose a user selecting a security rule and displaying information describing the selected rule, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981)." Page 2, paragraph 4.

Applicants agree that the proper standard for determining patentability under 35 U.S.C. §103 is based on "what the combined teachings of the references would have suggested to those of ordinary skill in the art," as alleged in the Office Action. Under such a standard, Applicants respectfully assert that the combined teachings of *Hayes* and *Shrader*, for at least the reasons discussed above, fail to suggest at least a "security application configured to... display information describing said selected rule ***in response to a selection of said one rule from said displayed list by said user***," as described by claim 1. (Emphasis added).

No Motivation to Combine

"When the patented invention is made by combining known components to achieve a new system, the prior art must (provide) a suggestion or motivation to make such a combination." *ALCO Standard Corp. v. Tennessee Valley Authority*, 808 F.2d 1490, 1498, 1 U.S.P.Q.2d 1337, 1343 (Fed. Cir. 1986). Moreover, in rejecting claim 1, it is asserted in the Office Action that:

> "It would have been obvious to one of ordinary skill in the art at the time the invention was made for the security application to be configured to enable said user to select one of said security rules and to display information describing said selected rule in response to a selection of said one rule by said user, since Shrader states at column 1, line 6 to column 2, line 2 that such a modification would be an improvement to the user interface, thereby making the interface user friendly by preventing an administrator from writing information down from a plurality of screens." Page 4, paragraph 12.

However, there is no cited deficiency in *Hayes* to motivate one of ordinary skill in the art to seek the alleged benefits described by *Shrader*. In particular, there is nothing to indicate that a user in *Hayes* suffers from having to write "information down from a plurality of screens." Thus, the proffered reasons for combining *Hayes* and *Shrader* are insufficient for establishing a *prima facie* case of obviousness. Indeed, where there is no apparent disadvantage present in a particular prior art reference, then generally there can be no motivation to combine the teaching of another reference with the particular prior art reference. *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349, 53 U.S.P.Q.2d 1580 (Fed. Cir. 2000). Thus, even if the alleged combination teaches all features of pending claim 1, as alleged in the Office Action, Applicants respectfully assert that the combination of *Hayes* and *Shrader* is improper, and the 35 U.S.C. §103 rejection of claim 1 should be overruled for at least this reason.

Discussion of 35 U.S.C. §103 Rejections of Claims 3 and 7

Claims 3 and 7 depend from claim 1, which is allowable for at least the reasons set forth above. Therefore, claims 3 and 7 are allowable as a matter of law. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988). Furthermore, claim 3 presently stands rejected in the final Office Action under 35 U.S.C. §103 as allegedly unpatentable over *Hayes* in view of *Shrader*. Claim 7 comprises similar claimed limitations which are missing from the alleged combination (with respect to the outstanding 35 U.S.C. §103 rejections) as claim 3. Therefore, claim 3 is discussed below as an exemplary claim for discussion.

Claim 3 reads as follows:

> 3. The system of claim 1, wherein said security application is configured to display said list within a window, said window including a plurality of selectable icons, ***said security application further configured to display different sets of information describing said selected rule in response to selections of different ones of said icons***. (Emphasis added).

Applicants respectfully assert that the combination of *Hayes* and *Shrader* fails to suggest at least the features of claim 3 highlighted above. Accordingly, the 35 U.S.C. §103 rejection of claim 3 is improper.

In this regard, it is alleged in the final Office Action that the "Members, Subgroups and Applet Permission" icons in Figure 17 of *Hayes* constitute the "selectable icons" recited by claim 1. However, selection of the "Members" and "Subgroups" icons do not result in the displaying of "information describing (a security) rule." In this regard, selection of the "Members" icon appears to result in the display of a list of "log-on identifications of all members that have been defined to the system." See column 19, lines 8-10. Further selection of the "Subgroups" icon appears to result in the display of "subgroups of the item selected in the left panel," which notably does not include any of the alleged "security rules." See column 19, lines 29-30. Moreover, only selection of the "Applet Permission" icon appears to result in a

display of information describing an alleged "security rule." Accordingly, the Office Action fails to establish that the cited art teaches a "security application further configured to display different sets of information describing said selected rule ***in response to selections of different ones of said icons***," as recited by claim 3. (Emphasis added).

For at least the above reasons, Applicants respectfully assert that the Office Action fails to establish a *prima facie* case of obviousness with respect to claim 3, and the 35 U.S.C. §103 rejection of this claim should be withdrawn.

Discussion of 35 U.S.C. §103 Rejections of Claims 9-11 and 13-17

Claim 9 presently stands rejected in the final Office Action under 35 U.S.C. §103 as allegedly unpatentable over *Hayes* in view of *Shrader*. Claims 10, 11, and 13-17 depend from claim 9. Therefore, claim 9 is discussed below as an exemplary claim for discussion.

For at least the reasons set forth above in the discussion of claim 1, Applicants respectfully assert that the "security application" allegedly taught by the combination of *Hayes* and *Shrader* is not configured to display "information describing (a) selected security rule in response to" a selection of the security rule. Moreover, Applicants assert that the cited art fails to provide a reason or motivation for "selecting one of said security rules from said displayed list" and "displaying information describing said selected rule in response to said selecting," as recited by claim 9. In addition, for at least the reason set forth above in the discussion of claim 1, Applicants respectfully submit that the combination of *Hayes* and *Shrader* is improper.

For at least the foregoing reasons, Applicants assert that the 35 U.S.C. §103 rejection of claim 9 is improper and should be overruled.

Discussion of 35 U.S.C. §103 Rejections of Claims 4 and 12

Claims 4 and 12 depend from claims 1 and 9, respectively, which are allowable for at least the reasons set forth above. Therefore, claims 4 and 12 are allowable as a matter of law. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988). Furthermore, claim 4 presently stands rejected in the final Office Action under 35 U.S.C. §103 as allegedly unpatentable over *Hayes* in view of *Shrader*. Claim 12 comprises similar claimed limitations which are missing from the alleged combination (with respect to the outstanding 35 U.S.C. §103 rejections) as claim 4. Therefore, claim 4 is discussed below as an exemplary claim for discussion.

Claim 4 reads as follows:

> 4. The system of claim 1, wherein said security application is configured to display a main window, ***said security application further configured to display rules of said list in a first sub-window of said main window and to display said information describing said selected rule in a second sub-window of said main window***. (Emphasis added).

Applicants respectfully assert that the combination of *Hayes* and *Shrader* fails to suggest at least the features of claim 4 highlighted above. Accordingly, the 35 U.S.C. §103 rejection of claim 4 is improper.

In rejecting claim 4, it is asserted in the Office Action that:

> "Regarding claims 4, 12, and 26, Hayes teaches said security application is configured to display a main window (Fig 17), said security application further configured to display rules of said list in a first sub-window (window of Members) of said main window and to display said information describing said selected rule in a second sub-window of said main window (window of Applet Permission)." Pages 4-5, paragraph 15.

However, the information displayed in response to selections of the "Members" icon and the "Applet Permission" icon are apparently displayed in the same window location (*i.e.*, in the scrollable sub-window shown on the right hand side of the main window depicted in Figures 15 and 17). See column 19, lines 8-10 and 50-55. Thus, the alleged "rules" and the alleged

"information describing said selected rule" do not appear to be displayed in ***different*** sub-windows. Further, *Shrader* does not remedy this deficiency of *Hayes*. Accordingly, the cited art fails to suggest "said security application further configured to display rules of said list in a first sub-window of said main window and to display said information describing said selected rule in a second sub-window of said main window," as recited by claim 4.

For at least the above reasons, Applicants respectfully assert that cited art fails to suggest each feature of claim 4, and the 35 U.S.C. §103 rejection of this claim should be overruled.

Discussion of 35 U.S.C. §103 Rejections of Claims 18, 21, and 22

Claims 18, 21, and 22 depend from a respective one of claims 1 and 9, which are allowable for at least the reasons set forth above. Therefore, claims 18, 21, and 22 are allowable as a matter of law. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988). Furthermore, claim 22 presently stands rejected in the final Office Action under 35 U.S.C. §103 as allegedly unpatentable over *Hayes* in view of *Shrader* and further in view of *Deo* (U.S. Patent No. 5,720,033). Claims 18 and 21 comprise similar claimed limitations which are missing from the alleged combination (with respect to the outstanding 35 U.S.C. §103 rejections) as claim 22. Therefore, claim 22 is discussed below as an exemplary claim for discussion.

Claim 22 recites "wherein said security application is configured to simultaneously display said first and second sub-windows." Applicants respectfully assert that the combination of *Hayes* and *Shrader* fails to suggest at least the foregoing features of claim 22. Accordingly, the 35 U.S.C. §103 rejection of claim 22 is improper.

In this regard, claim 22 includes the features of its base claim 4. In rejecting claim 4, it is alleged in the Office Action that the information displayed in response to the "Members" icon and the "Applet Permission" icon respectively constitute the "rules of said list" and the

"information describing said selected rule" recited by claim 4. As described above in the arguments for allowance of claim 4, such information is displayed at the same window location and is, therefore, not displayed "simultaneously." Accordingly, *Hayes* fails to teach and, in fact, teaches against at least the features of "wherein said security application is configured to ***simultaneously*** display said first and second sub-windows," as described by claim 22. (Emphasis added). Further, *Shrader* and *Deo* fail to remedy this deficiency of *Hayes*.

In this regard, in rejecting claim 22, it is alleged in the Office Action that *Deo* teaches "wherein said displaying rules of said list in a first sub-window (Figure 1 [block 14]; column 8, lines 3-19)." However, Figure 1 of *Deo* does not appear to describe or show any "windows." Rather, Figure 1 of *Deo* appears to be a block diagram depicting the primary components of a security platform. See column 6, lines 8-9. Further, the cited section at column 8 of *Deo* describes populating the file 14 with data, but does not describe the manner in which the data of the file 14 is ***displayed***. Moreover, there is nothing in *Deo* that suggests the information relating to the "Members" icon and the "Applet Permission" icon of *Hayes* should be ***simultaneously*** displayed in ***different*** sub-windows, as described by claim 22 and its base claim 4.

In addition, Applicants respectfully assert that the ***cited art*** fails to provide a sufficient motivation for combining *Deo* with *Hayes* and *Shrader*, and the alleged combination of *Hayes*, *Shrader*, and *Deo* is, therefore, improper.

In this regard, in rejecting claim 22 it is alleged in the Office Action that:

> "It would have been obvious to one of ordinary skill in the art at the time the invention was made to display the list of rules in a separate window, since *Deo* states at column 8, lines 3-19 that such a modification would allow a user to add, edit and change rules as they applied to various applications." Page 7, paragraph 28.

However, there is nothing to suggest that the alleged combination of *Hayes* and *Shrader* suffers from any deficiency that would be alleviated by the alleged benefit of *Deo*. In this regard, the

alleged motivation for combining *Deo* with *Hayes* and *Shrader* is apparently to allow a user to "add, edit and change rules," but, in *Hayes*, it appears that a user can "add, edit, and change" the alleged "list of rules" (*i.e.*, the list 1720 shown in Figure 17 of *Hayes*). See, *e.g.*, column 19, lines 55-58, and column 20, lines 48-51. Thus, Applicants submit that the proffered reason for combining *Deo* with *Hayes* and *Shrader* is not sufficiently supported by the cited art and is, therefore, insufficient under 35 U.S.C. §103.

For at least the above reasons, Applicants respectfully assert that the cited art fails to suggest each feature of claim 22 and the alleged combination of *Hayes*, *Shrader*, and *Deo* is improper. Accordingly, the 35 U.S.C. §103 rejection of claim 22 should be overruled.

Discussion of 35 U.S.C. §103 Rejection of Claim 23

Claim 23 presently stands rejected in the final Office Action under 35 U.S.C. §103 as allegedly unpatentable over *Hayes* in view of *Shrader*. For at least the reasons set forth above in the discussion of claim 1, Applicants respectfully assert that the "security application" allegedly taught by the combination of *Hayes* and *Shrader* is not configured to display "information describing (a) selected security rule in response to" a selection of the security rule. Moreover, Applicants assert that the cited art fails to provide a reason or motivation for combining "logic for enabling a user to make a selection of one of said security rules while said list of security rules, including said one security rule, is being displayed" and "logic for displaying information describing said selected rule in response to said selection," as recited by claim 23. In addition, for at least the reason set forth above in the discussion of claim 1, Applicants respectfully submit that the combination of *Hayes* and *Shrader* is improper.

For at least the foregoing reasons, Applicants assert that the 35 U.S.C. §103 rejection of claim 23 is improper and should be overruled.

Discussion of 35 U.S.C. §103 Rejections of Claims 24-27

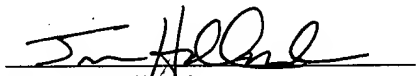
Each of the claims 24-27 depend from claims 1, 4, and 22. Since claims 1, 4, and 22 are allowable for at least the reasons set forth above, claims 24-27 are allowable as a matter of law. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988). Further, the Office Action appears to admit that all of the features of claim 22 are not disclosed by the combination of *Hayes* and *Shrader*, since claim 22 is rejected as allegedly unpatentable over the combination of *Hayes*, *Shrader*, ***and Deo***. Claims 24-27 include all of the features of claim 22 but are rejected as allegedly unpatentable over the combination of *Hayes* and *Shrader*. If the combination of *Hayes* and *Shrader* fails to suggest each feature of claim 22, it is unclear how the combination of *Hayes* and *Shrader* can be sufficient for rejecting claims 24-27, which include the features of claim 22. In addition, for at least the reasons set forth above in the discussion of claim 22, Applicants submit that *Deo* fails to remedy the deficiencies of *Hayes* and *Shrader*. For at least the foregoing reasons, Applicants respectfully assert that the Office Action fails to establish a *prima facie* case of obviousness with respect to claims 24-27.

CONCLUSION

Based on the foregoing discussion, Applicants respectfully request that the Examiner's final rejections of claims 1-28 be overruled and withdrawn by the Board, and that the application be allowed to issue as a patent with all pending claims.

Respectfully submitted,

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.

By: 

Jon E. Holland
Reg. No. 41,077
(256) 704-3900 Ext. 103

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

VIII. CLAIMS - APPENDIX

1. A computer system, comprising:

memory; and

a security application configured to display a list of security rules for locking down resources of said computer system, said security application configured to enable a set of said security rules, based on inputs from a user, and to cause said computer system to enforce said enabled set of security rules by modifying a machine state of said computer system, said security application further configured to enable said user to select one of said security rules and to display information describing said selected rule in response to a selection of said one rule from said displayed list by said user, said information based on data stored in said memory.

2. The system of claim 1, wherein said security application is configured to display said information immediately in response to said selection.

3. The system of claim 1, wherein said security application is configured to display said list within a window, said window including a plurality of selectable icons, said security application further configured to display different sets of information describing said selected rule in response to selections of different ones of said icons.

4. The system of claim 1, wherein said security application is configured to display a main window, said security application further configured to display rules of said list in a first sub-window of said main window and to display said information describing said selected rule in a second sub-window of said main window.

5. The system of claim 4, wherein said security application is configured to categorize said list of rules, said security application further configured to display categories of said rules in a third sub-window of said main window.

6. The system of claim 5, wherein said security application is configured to enable said user to select one of said categories and is configured to display, in said first sub-window, rules of said list that are associated with one of said categories presently selected by said user.

7. The system of claim 6, wherein said main window includes a plurality of selectable icons, said security application further configured to display in said second sub-window different sets of information describing said selected rule in response to selections of different ones of said icons.

8. A computer system, comprising:

means for displaying a list of security rules for locking down resources of said computer system;

means for receiving inputs from a user of said computer system;

means for enabling a set of said security rules based on said inputs from said user;

means for enforcing said enabled set of security rules;

means for selecting one of said security rules from said displayed list; and

means for displaying information describing said selected rule in response to a selection of said one rule by said selecting means.

9. A method for locking down resources of computer systems, comprising:

displaying a list of security rules for locking down resources of a computer system;

receiving inputs from a user of said computer system;

enabling a set of said security rules based on said inputs from said user;

enforcing said enabled set of security rules;

selecting one of said security rules from said displayed list; and

displaying information describing said selected rule in response to said selecting.

10. The method of claim 9, wherein said displaying said information is performed immediately in response to said selecting.

11. The method of claim 9, wherein said displaying said information further includes displaying said information within a window, said window having selectable icons, said method further comprising:

selecting one of said icons; and

displaying other information describing said selected rule in response to said selecting one of said icons.

12. The method of claim 9, wherein said displaying a list of security rules further comprises displaying rules of said list in a first sub-window of said main window, and wherein said displaying information further comprises displaying said information describing said selected rule in a second sub-window of said main window.

13. The method of claim 12, further comprising:

categorizing said list of rules; and

displaying categories of said rules in a third sub-window of said main window.

14. The method of claim 13, further comprising:

selecting one of said categories,

wherein said displaying a list of security rules includes displaying, in said first sub-window and in response to said selecting one of said categories, rules of said list that are associated with said one category.

15. The method of claim 14, wherein said displaying said main window includes displaying a plurality of selectable icons, and wherein said method further comprises:

selecting one of said icons; and

displaying, in said second sub-window, other information describing said selected rule in response to said selecting one of said icons.

16. The method of claim 9, wherein said selecting is performed while said list of security rules, including said one security rule, is being displayed via said displaying a list of security rules.

17. The method of claim 11, wherein said selecting is performed while said list of security rules, including said one security rule, is being displayed via said displaying a list of security rules.

18. The method of claim 12, wherein said displaying rules of said list in a first sub-window and said displaying said information describing said selected rule in a second sub-window are performed simultaneously.

19. The system of claim 1, wherein said selection of said one rule occurs while said one rule is being displayed to said user.

20. The system of claim 3, wherein said selection of said one rule occurs while said one rule is being displayed to said user.

21. The system of claim 3, wherein said security application is configured to simultaneously display said list in a first sub-window of said window and one of said sets of information in a second sub-window of said window.

22. The system of claim 4, wherein said security application is configured to simultaneously display said first and second sub-windows.

23. A computer-readable medium having a program, the program comprising:

logic for displaying a list of security rules;

logic for enabling a set of said security rules, based on inputs from a user;

logic for causing a computer system to enforce said enabled set of security rules;

logic for enabling a user to make a selection of one of said security rules while said list of security rules, including said one security rule, is being displayed; and

logic for displaying information describing said selected rule in response to said selection.

24. The system of claim 22, wherein said information comprises help information for informing said user of an operational ramification to said system of enabling said one rule.

25. The system of claim 24, wherein said security application is configured to display a plurality of selectable icons simultaneously with said information, said security application further configured to display new information describing said one rule based on said selection of said one rule and in response to a selection of one of said icons by said user.

26. The system of claim 25, wherein said security application is configured to display said selectable icons in said second sub-window.

27. The system of claim 26, wherein said security application is configured to categorize said list of rules and to display categories of said rules in a third sub-window of said main window.

28. The system of claim 1, wherein said information comprises help information for informing said user of an operational ramification to said system of enabling said one rule.

IX. EVIDENCE - APPENDIX

None.

X. RELATED PROCEEDINGS - APPENDIX

None.